BEEKEEPER

White Paper

# DATA SECURITY

# OUTLINE



*"We manage risk with the highest standards of security tools and processes to ensure your right to privacy."*

**Dr. Amir Ameri, LL.M.**
Certified ISO 27001 Internal Auditor
Chief Risk Compliance Officer, Group Data Protection Officer

# STATEMENT OF COMMITMENT TO INFORMATION SECURITY

The Beekeeper product and services are delivered to many companies and the public sector in a variety of market segments across the globe. Our customers entrust their data security and privacy to us, and all Beekeeper employees in return provide full commitment to maintain this trust.

Senior management, including Beekeeper's Data Protection Officer Dr. Amir Ameri, supports all necessary information security tools and processes. We maintain our commitment without compromising seamless delivery of the Beekeeper product and services, while maintaining confidentiality, integrity, and availability of our customers' data.

To achieve the highest level of our customer's trust and to further expand our commitment, we have implemented an ISMS (Information Security Management System) in accordance with the internationally-recognized data privacy best practices as outlined by the ISO 27001:2013 certification process, including ISO 27017:2015 and ISO 27018:2019.

The enclosed documentation is an attestation to our commitment to customer data protection. Beekeeper will remain vigilant and relentless in continuously improving our ISMS and maintaining our data privacy commitment to our customers and employees in the future.

CEO: Dr. Cristian Grossmann


CTO: Flavio Pfaffhauser


DPO: Dr. Amir Ameri

# PILLARS OF SECURITY

Beekeeper considers data confidentiality, integrity, and availability a top priority. We demonstrate our commitment to continuous customer data protection and data privacy processes in the following ways:

1. Beekeeper uses industry-proven data security technologies and practices, such as certified data centers to protect data.
2. Beekeeper continuously evaluates our product internally for vulnerabilities, and regular penetration testing is performed by external security specialists.
3. Beekeeper's 24/7 on-call technical support ensures rapid response time to any new threats.
4. Beekeeper adheres to industry standards for Information Security Control Objectives as defined by the International Organization for Standardization.
5. Beekeeper undergoes both internal and external audits on a regular basis.

Beekeeper's data security practices are in accordance with the six information security pillars to the right. Each pillar contributes to the use of advanced security technology and controls, and in combination, meet the requirements of our ISMS (Information Security Management System). This is congruent with and beyond the requirements of the stringent accreditation process as verified by our ISO 27001:2013 in addition to ISO 27017:2015 and ISO 27018:2019 certifications.

**Virtual Private Cloud (VPC)**

**Multi-Tenant Architecture**

**Closed Company User Group and Customer Controls Access**

**Full Encryption**

**Compliance with GDPR and Certified to ISO 27001, 27017, 27018**

**Availability**

### Virtual Private Cloud (VPC)

Beekeeper operates a Virtual Private Cloud in each of its certified data centers, restricted to that particular jurisdiction of the VPC where the customer has chosen their data storage. Starting with the border firewall to the VPC, and all other systems within the VPC, all are maintained and operated by Beekeeper employees only.

The Swiss Federal Data Protection Information Commissioner states the following about VPCs in their cloud-computing guide: *"In the case of a **private** cloud, the situation is different; this is run by the enterprise or by a third party and is always set up solely for the use of the enterprise itself. Such a system is much more secure."*

### Multi-Tenant Architecture

Beekeeper's standard SaaS offering is a customer database on a multi-tenant architecture, with numerous embedded security controls on multiple logical layers including the application layer. This allows for efficient and secure sharing of physical resources such as the CPU. Beekeeper's SaaS offering may also be utilized as a single tenant solution with the impacted financial difference of utilizing separate physical resources.

### Closed Company User Group and Customer Controls Access

Beekeeper was built as an internal communication platform. Access provisioning is fully controlled by the customer to their tenant. Only administrative roles via the Beekeeper dashboard or automated control processes such as the active directory sync allows control over identity management.

### Full Encryption

Beekeeper utilizes cryptographic measures in various use cases, including encryption of all internal communication channels as well as encryption of data at rest, regardless of whether data is in storage facilities or the end user's mobile device.

### Compliance with GDPR and Certified to ISO 27001, ISO 27017, and ISO 27018

Beekeeper maintains compliance with the General Data Protection Regulation (GDPR) as outlined for the protection of personal data,

as well as other jurisdictionally-mandated data privacy requirements. Beekeeper has implemented an ISMS framework in accordance with ISO 27001 control objectives and attained ISO 27001:2013 certification. Beekeeper's data processing agreement is a contractual agreement between Beekeeper and its customers, outlining all requirements in this aspect. In addition, certification for ISO 27017:2015 and ISO 27018:2019 have been achieved. These latter security standardizations allow Beekeeper to demonstrate compliance as a SaaS offering both as a Cloud Service Provider, as well as when processing personal data in cloud solutions.

### Availability

Beekeeper agrees to a 99.9% availability with customers as part of its commercial subscription agreement contract. Respectively, Beekeeper fulfills this obligation with multiple redundancy and frequent testing of its service availability, performed on a quarterly basis.

# BEEKEEPER'S ISO CERTIFICATIONS

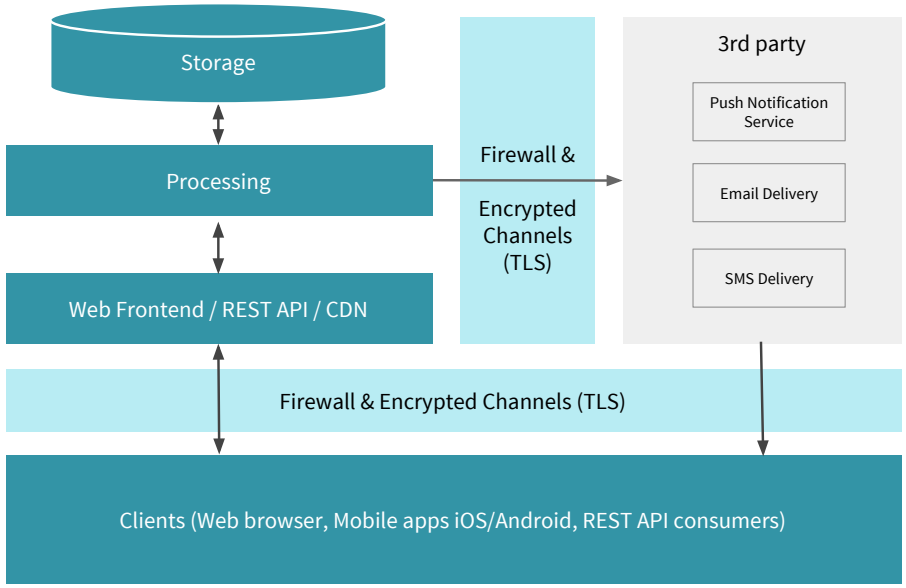
The International Organization for Standardization is an independent, non-governmental organization, the members of which are the standards organizations of the 164 member countries. ISO 27001 is a set of information security and data privacy best practices regarding the management of customer data that adheres to the highest international data security standards. Importantly, ISO standards are the result of a consensus-driven process by experts from all over the world, pooling vast international experience and knowledge from all business sectors.

Data that falls under the risk management controls set in place by ISO 27001 include financial information, intellectual property, a customer's or employee's details, or any personal information entrusted to us. In addition, ISO 27017 & ISO 27018 certifications establish the framework of Control Objectives to operate as a Cloud Service Provider, as well as process Personal Data in a Cloud Based Solution.

Learn more about Beekeeper's journey to ISO 27000 series certification, ongoing adherence to IS0 27001, 27017, 27018 information security standards, and FAQs.



# ARCHITECTURE




As a cloud-based team app, we maximize the security of our platform using a layered approach. Operating in our own virtual private cloud (recognized as the most secure implementation for cloud-based solutions) each VPC is implemented independent of other Beekeeper VPCs.

**Storage:** Data is stored in a state-of-the-art relational database and indexed by a separate database system.

**Multi-tenancy:** We operate our database as a multi-tenant environment. Each of our customers is defined as an independent tenant with segregation from other customer data.

**Processing:** Incoming and outgoing data is processed by our own code. We use a message queuing system for asynchronous request processing.

**Notifications (via third-party systems):** Push notifications, emails and SMS text messages are sent via third-party providers. All connections to third-party systems are secured via TLS.

# ACCESS TO BEEKEEPER

Beekeeper can be accessed through a number of digital interfaces. Each interface provides security settings that both protect user data while ensuring accessibility.

**Web browsers:** Browsers only store a secure cookie which authenticates the current user. There is no local storage of customer data via this interface.

**Mobile apps:** On Android and iOS, access credentials are stored in the encrypted containers that the OS (operating system) provides.

**Custom REST API:** Beekeeper has developed a REST API and provides documentation to highlight best security practices when programming custom clients.

## Connections to Beekeeper

All connections to Beekeeper are over HTTPS (TLS 1.2 and 1.3 only). Any attempt to connect over HTTP is redirected to HTTPS.

## Certified Data Centers

Beekeeper only uses certified data center service providers that have obtained internationally-recognized and approved compliance certifications for information security management:

- **Amazon Web Services:** aws.amazon.com/compliance
- **Interoute** (phasing out 2020): gtt.net/nl-en/company/security-and-compliance
- **Google:** cloud.google.com/security/compliance



# SECURITY AUDITS AND PENETRATION TESTING

### External

Beekeeper's information security policy mandates independent external security firms to perform annual penetration tests of Beekeeper. All findings are recorded in our risk inventory, and mitigation steps are defined and implemented in accordance to our change management process.

### Internal

The following internal automated vulnerability checks are performed:

- Independent of code changes:
  - » Daily SSL Certificate check
  - » Weekly configuration scanning, activity monitoring, and reviewing against best practices library
  - » Weekly dynamic application security testing

- For every code change:
  - » Mandatory peer review
  - » Static application security testing
  - » Unit and integration test suites focused on access permissions
  - » System library vulnerability checks

# DEVELOPMENT CYCLE

Derived in accordance with ISO 27001 control objectives, the information security policy of Beekeeper mandates a strict segregation of duties, as well as separated environments. Listed below, these separated environments for the development life cycle maximize the confidentiality, integrity and availability of our information systems.

**Environments:**

- Production
- Staging
- Development

**Roles:**

- Requester
- Approver
- Reviewer/implementer

# ACCESS CONTROL

Beekeeper considers access control as consisting of two key components:

- Authentication
- Authorization

For managing access control requirements, Beekeeper has developed its own proprietary systems and interfaces, as well as a control dashboard.

### Authentication

For internal processes, as governed by the requirements stated in our Beekeeper product and services access control principles, Beekeeper requires two-factor authentication for its employees.

For customer access, Beekeeper is able to maintain compliance with company policy where two-factor authentication is available through a single sign-on solution (SSO). Beekeeper is also able to connect to the company active directory, as well as consider any other type of authentication mechanism.

### Authorization

Beekeeper has developed its own proprietary authorization server, which is utilized for provisioning rights to Beekeeper systems. Some features of Beekeeper's authorization capabilities are available to the customer-defined administrator through the Beekeeper dashboard.

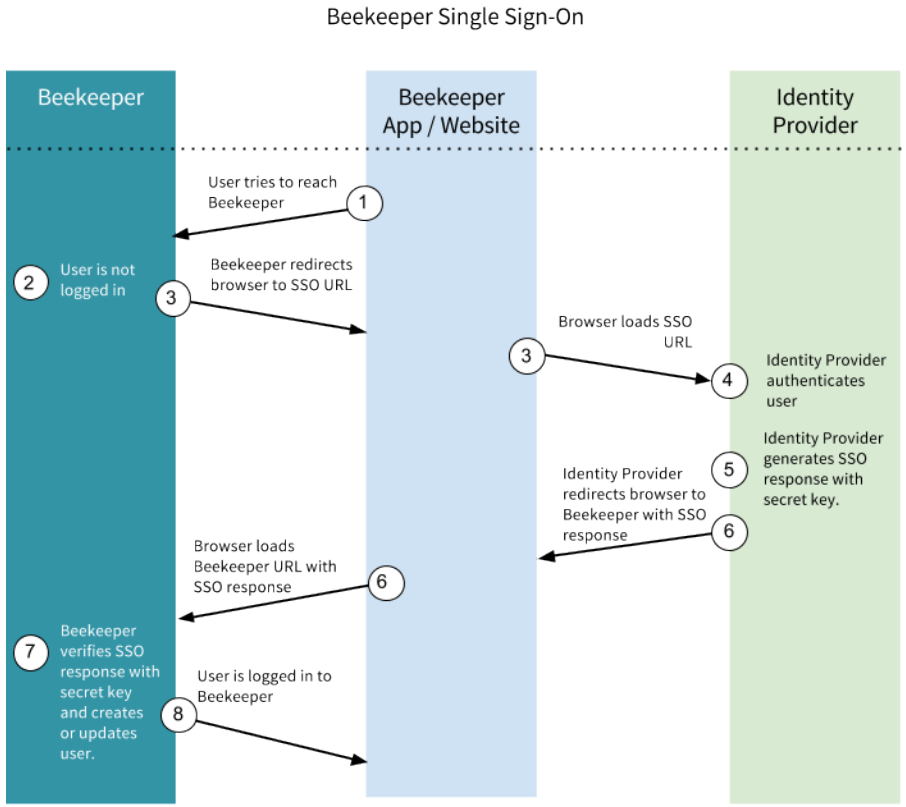
## Beekeeper Dashboard

Company-defined administrators may use the Beekeeper dashboard via secure internal communication channels to control the following user administrator functions:

- Create, update, or delete a user
- Logout an active user
- Suspend user access
- Configure SAML single sign-on
- Bulk import and update users from an Excel file

## Data Preservation and Recovery

In accordance with ISO 27001 control objectives for business continuity and disaster recovery, Beekeeper utilizes data preservation managed services by its certified data center providers. Our solutions are architected with full redundancy capabilities and tested numerous times throughout the year (at least quarterly). Encryption at rest is implemented for all backup systems as well.



# PRODUCT USE SECURITY FEATURES

- **Authentication**
  - » Login using email, phone number, or username in combination with the password
  - » Preset “password strength” (8 or more characters, upper and lowercase letters, and at least one number)
  - » Admins can reset passwords. After the first login there’s a request to change the password. When resetting the password, you cannot use a former password
  - » Auto logout users after X days (number is set by administrators)
  - » Login to mobile via QR code. Alert by email about login via a one-time QR code
  - » Admins can log out users and suspend accounts
  - » The logout made by an admin will logout the user from every single device
  - » Account is locked after 10 unsuccessful login attempts

- **Authorization**
  - » Every user has a role assigned, which defines what someone can do within the application (see the Roles section).

- **Session timeout**
  - » Session timeouts can be configured in the event users access Beekeeper from public computers.

- **User suspension**
  - » Administrators can suspend users at any point. A suspended user will be immediately logged out of all clients and will lose access to all data. The data of a suspended user is retained and can be made available for forensic investigations.

- **Denylist/allowlist email domains from login**

- **Single Sign-On (SAML)**

- **Alert by email when logging in on a previously unknown device**

- **Backup**
  - » Regular backups of user information and all data are maintained to prevent accidental or malicious destruction

- **Roles**
  - » Available roles: Global Admin, Org. Unit Admin, Location Admin, Group Admin, Stream Admin, and Content Moderator. Learn more in the Help Center.

- **Activity monitor available through the Meta Dashboard (customer must request data access to see this information)**
  - » Possible to see last login with device information
  - » List with devices used to log in

- **Antivirus to scan files sent within the Beekeeper platform**

- **Disallow or restrict possibility of embedding the application within another page**

# FREQUENTLY ASKED QUESTIONS

***Q*:** Can data and messages be exported for internal archiving or reviewing?
***A:*** Yes, based on a defined process, Beekeeper may give access to the data for automated archiving purposes.

***Q:*** Are security penetration test reports available for review?
***A:*** Yes, upon request we can share the reports of previous penetration tests.

***Q:*** Is Beekeeper hosted on a shared cloud infrastructure?
***A:*** Yes, but our certified data centers offer virtual private cloud (VPC) features to guarantee data isolation from other Beekeeper customers.

***Q:*** Do you offer on-premise hosting?
***A:*** We do not offer on-premise hosting.

***Q:*** Is an audit log available?
***A:*** An audit log can be made available in CSV format.

***Q:*** Is Beekeeper's product and services HIPAA Security Compliant?
***A:*** Beekeeper's product and services meet the requirements outlined by HIPAA Security Controls, by having implemented an ISMS (Information Security Management System) that is certified according to information security best practices outlined by the ISO accreditation body.
It is important to note that Beekeeper is an internal communication platform and not a healthcare data processing platform.

***Q:*** How is Beekeeper's support and maintenance?
***A:*** As a SaaS offering, Beekeeper's product is supported and maintained from Beekeeper's Zurich-Switzerland and Krakow-Poland Support Centers. Beekeeper also provides local help desk support services from its offices in the US and Germany-EU.

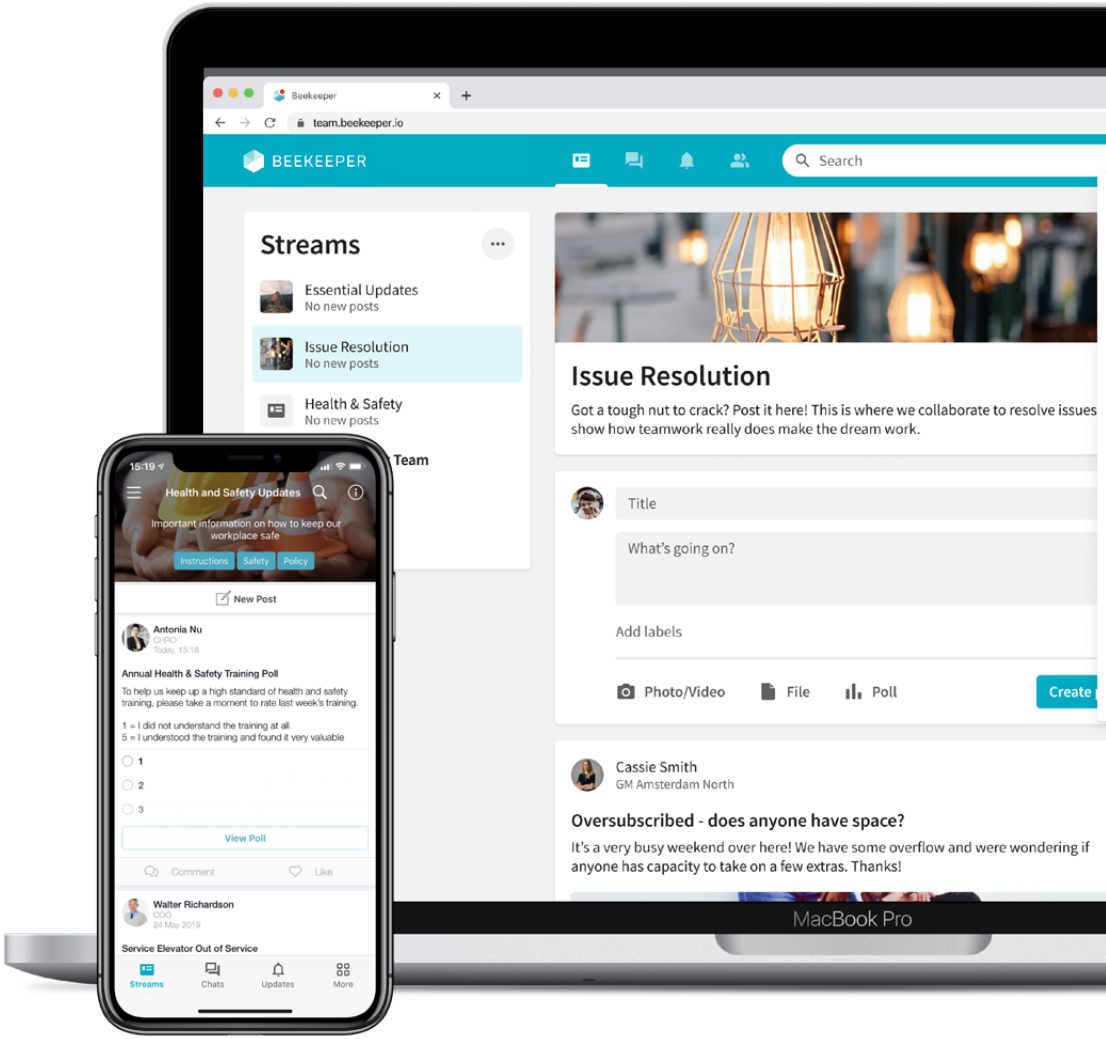
**Contact Us**
If you have further security related questions, contact us at security@beekeeper.io.

# ABOUT BEEKEEPER

Beekeeper's mobile platform is the single point of contact for your frontline workforce. With all communications and tools in one place, Beekeeper empowers frontline employees to be more agile, more productive, and create a safer workplace.

Our secure platform offers a consumer-grade employee experience at the scale you need. Deskless workers can check resources and share best practices in real time. Managers can resolve issues quickly, handle non-routine work efficiently, and track team performance. Executives can increase business resilience and agility in uncertain times. Integrate seamlessly with your existing systems to create the future, now.

Get Started




**For more detailed security information and FAQs, visit beekeeper.io/security.**

Release Date (R2.0): August, 2020